

## CLAIMS

We claim:

1 1. A method of identifying the entry point of an attack upon a device protected by an intrusion  
2 detection system, the method comprising the steps of:

3 obtaining intrusion information regarding an attack upon a device protected by an  
4 intrusion detection system;

5 obtaining network information regarding the attack upon the device; and

6 determining a portal of the attack upon the device by correlating the intrusion information  
7 and the network information.

1 2. The method of claim 1, wherein the portal of the attack is an entry point of the attack.

1 3. The method of claim 1, wherein the portal of the attack is an exit point of the attack.

1 4. A method of identifying the entry point of an attack upon a device protected by an intrusion  
2 detection system, the method comprising the steps of:

3 obtaining intrusion information, from an intrusion detection system, regarding an attack  
4 upon a device protected by the intrusion detection system;

5 obtaining network information, from network equipment connected to the device,  
6 regarding the attack upon the device; and

7 determining a portal of the attack upon the device using a correlation engine to correlate  
8 the intrusion information and the network information.

1 5. A method of identifying the entry point of an attack upon a device protected by an intrusion  
2 detection system, the method comprising the steps of:

3 obtaining intrusion information, from an intrusion detection system, regarding an attack  
4 upon a device protected by the intrusion detection system;

5 obtaining network information, from network equipment connected to the device,  
6 regarding the attack;

7 determining a logical entry point of the attack using a correlation engine to correlate the  
8 intrusion information and the network information; and

9 identifying a physical entry point associated with the logical entry point.

1 6. The method of claim 5, wherein the intrusion information includes an address.

1 7. The method of claim 5, wherein the address is a source address.

1 8. The method of claim 5, wherein the address is a destination address.

1 9. The method of claim 5, wherein the network information includes a logical port identifier of a  
2 logical port associated with the address.

1 10. The method of claim 9, wherein the step of determining a logical entry point includes the  
2 step of finding, in the network data, the logical port identifier of the logical port associated with  
3 the address.

1 11. The method of claim 9, wherein the step of identifying a physical entry point includes the  
2 step of identifying a physical port associated with the logical port.

1 12. The method of claim 5, wherein the network equipment includes a network router.

1 13. The method of claim 12, wherein the physical entry point includes a physical port of the  
2 network router.

1 14. The method of claim 12, wherein the logical entry point includes a logical port of the  
2 network router.

1 15. The method of claim 5, wherein the network equipment includes a firewall with routing  
2 function.

1 16. The method of claim 5, wherein the network equipment includes a network dispatcher.

1 17. The method of claim 5, wherein the network equipment includes a load balancer.

1 18. The method of claim 5, wherein the intrusion detection system includes network based  
2 intrusion detection equipment.

1 19. The method of claim 5, wherein the intrusion detection system includes host based intrusion  
2 detection equipment.

1 20. The method of claim 5, wherein the intrusion detection system includes application based  
2 intrusion detection equipment.